



Agilent E6640A EXM Wireless Test Set

Security Features and Document of Volatility



Agilent Technologies

Notices

© Agilent Technologies, Inc. 2014

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Agilent Technologies, Inc. as governed by United States and international copyright laws.

Trademark Acknowledgements

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Adobe Acrobat® and Reader® are U.S. registered trademarks of Adobe Systems Incorporated.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

MATLAB® is a U.S. registered trademark of Math Works, Inc.

Norton Ghost™ is a U.S. trademark of Symantec Corporation.

Wikipedia® is a registered trademark of the Wikimedia Foundation.

Manual Part Number

E6640-90005

Print Date

January, 2014

Printed in USA

Agilent Technologies Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as “Commercial computer software” as defined in DFAR 252.227-7014

(June 1995), or as a “commercial item” as defined in FAR 2.101(a) or as “Restricted computer software” as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Agilent Technologies’ standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A **WARNING** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Warranty

This Agilent technologies instrument product is warranted against defects in material and workmanship for a period of one year from the date of shipment. During the warranty period, Agilent Technologies will, at its option, either repair or replace products that prove to be defective.

For warranty service or repair, this product must be returned to a service facility designated by Agilent Technologies. Buyer shall prepay shipping charges to Agilent Technologies, and Agilent Technologies shall pay shipping charges to return the product to Buyer. For products returned to Agilent Technologies from another country, Buyer shall pay all shipping charges, duties, and taxes.

Where to Find the Latest Information

Documentation is updated periodically. For the latest information about these products, including instrument software upgrades, application information, and product information, see the following URLs:

<http://www.agilent.com/find/e6640a>

To receive the latest updates by email, subscribe to Agilent Email Updates:

<http://www.agilent.com/find/emailupdates>

Information on preventing instrument damage can be found at:

<http://www.agilent.com/find/tips>

Is your product software up-to-date?

Periodically, Agilent releases software updates to fix known defects and incorporate product enhancements. To check for software updates for your product, go to the Agilent Technical Support website at:

http://www.agilent.com/find/e6640a_software

1 Table of Contents

2. Contacting Agilent Sales and Service Offices	7
3. Products Covered by this Document	9
4. Security Terms and Definitions	11
5. Instrument Memory & Document of Volatility	13
Memory in the Controller	14
Memory in the Frequency Reference	15
Memory in the TRX	16
6. Memory Clearing, Sanitization and/or Removal Procedures	19
Instrument Sanitization Procedures	20
Removable Hard Drive Data Destruction	20
Hard Drive Removal	20
Application License Key Storage	21
Other Memories	22
7. User and Remote Interface Security Measures	23
SCPI/GPIB Control of Interfaces	23
Operating System Security Features	23
Determining the Test Set's Operating System	24
USB Interfaces	24
Disabling or Enabling Autorun/Autoplay	24
Windows 7	24
Windows XP	25
Registry Key Definitions	25
Disable & Enable Procedure	26
Microsoft AutoRun Patch	28
More Information	28
Configuring USB for Read-only	28
8. Procedure for Declassifying a Faulty Instrument	31
Appendix A. References	33



2 Contacting Agilent Sales and Service Offices

Assistance with test and measurement needs, and information to help you find a local Agilent office, is available via the internet at, <http://www.agilent.com/find/assist>. If you do not have internet access, please contact your designated Agilent representative.

NOTE

In any correspondence or telephone conversation, refer to the instrument by its model number and full serial number. With this information, the Agilent representative can determine whether your unit is still within its warranty period.



3 Products Covered by this Document

Product Name**Model Numbers**

EXM Wireless Test Set

E6640A

This document describes instrument memory types and security features. It provides a statement regarding the volatility of all memory types, and specifies the steps required to declassify an instrument through memory clearing, sanitization, or removal.

For additional information, go to:

<http://www.agilent.com/find/security>

IMPORTANT

Be sure that all information stored by the user in the instrument that needs to be saved is properly backed up before attempting to clear any of the instrument memory. Agilent Technologies cannot be held responsible for any lost files or data resulting from the clearing of memory.

Be sure to read this document entirely before proceeding with any file deletion or memory clearing.

Products Covered by this Document



4 Security Terms and Definitions

Term	Definition
Clearing	As defined in Section 8-301a of DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM)” , clearing is the process of eradicating the data on media before reusing the media so that the data can no longer be retrieved using the standard interfaces on the instrument. Clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.
Instrument Declassification	A term that refers to procedures that must be undertaken before an instrument can be removed from a secure environment, such as is the case when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both. Agilent declassification procedures are designed to meet the requirements specified in DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM)” , Chapter 8.
Sanitization	<p>As defined in Section 8-301b of DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM)”, sanitization is the process of removing or eradicating stored data so that the data cannot be recovered using any known technology. Instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment, such as when it is returned to the factory for calibration.</p> <p>Agilent memory sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are specified in the “Clearing and Sanitization Matrix” in Appendix O of the ODAA Process Guide for C&A of Classified Systems under NISPOM.</p>
Secure Erase	Secure Erase is a term that is used to refer to either the clearing or sanitization features of Agilent instruments.



5 Instrument Memory & Document of Volatility

This chapter summarizes all memory types in the instrument.

The descriptions are divided between:

1. [Memory in the Controller](#),
2. [Memory in the Frequency Reference](#).
3. [Memory in the TRX](#).

Memory in the Controller

This section contains information on the memory components used in the controller.

The table provides details of the size of each memory component, its type, how it is used, its location, volatility, and the sanitization procedure.

NOTE The instrument contains no user-accessible non-volatile memory, except for the SSD listed as the second item in the table below. For this reason, as indicated in the tables below, no sanitization procedure is required for any memory component except the SSD..

Table 5-1 Summary of controller instrument memory

Memory Component, Type and Size	User Modifiable (Y/N)?	Volatile (Y/N)?	Purpose/Contents/Remarks	Location in Controller	Sanitization Procedure
Main memory (RAM) 4GB or 8GB Std.	Yes	No	Windows Operating System memory. Data input from user, operating system.	Motherboard	Cycle power. This is volatile memory.
Media Storage 160 GB Solid State Drive	Yes	Yes	Windows Operating System boot device and user files including saved programs, data, settings, images, license files, etc. Data (Operating System) is factory installed; other data is user-saved.	Motherboard	Remove the drive; see instructions below.
Flash memory for BIOS (non-volatile memory)	No	Yes	Contains default BIOS settings for use when booting the controller. Programmed at factory or during BIOS upgrade. Settings may be toggled by user. Contains no user data.	Motherboard	None
DDR2-533 memory	No	No	Video RAM	Motherboard	Cycle power. This is volatile memory.

Memory in the Frequency Reference

This section contains information on the memory components used in the M9300A PXIe Frequency Reference.

The table provides details of the size of each memory component, its type, how it is used, its location, volatility, and the sanitization procedure.

Table 5-2 Summary of frequency reference instrument memory

Memory Component, Type and Size	User Modifiable (Y/N)?	Volatile (Y/N)?	Purpose/Contents/Remarks	Location in Controller	Sanitization Procedure
1. Flash Memory 128 Mbit	No	No	Stores Module Model Number, Serial Number, Manufacturing Number, PCB Part and Version Numbers, Cal Verify Date, Max Module Temperature, and Calibration Data.	Reference PC board	None; this is not user accessible.
2. Flash Memory 128 Mbit	No	No	Device firmware. Images can be changed using the Agilent Soft Front Panel firmware update utility.	Reference PC board	None; this is not user accessible.
3. Flash Memory 128 Mbit	Yes	No	Stores Calibration Preferences: Due Date, Subject to Periodic Cal, Module Cal Warnings, Cal Due Reminder, Module Cal Reminder and Passphrase.	Reference PC board	All values can be reset using the Soft Front Panel.
4. FPGA	Yes	Yes	Reference Output selections, External Reference and Frequency selections, Time Shift and Self Test results.	Reference PC board	Cycle power.
5. Flash Memory 128 Mbit	Yes	Yes	Stores User Customizable Asset Number and System Identification.	Reference PC board	All values can be reset using IVI driver.

Memory in the TRX

This section contains information on the memory components available in your instrument.

The table provides details of the size of each memory component, its type, how it is used, its location, volatility, and the sanitization procedure.

Table 5-3 Summary of TRX instrument memory

Memory Component, Type and Size	User Modifiable (Y/N)?	Volatile (Y/N)?	Purpose/Contents	Location in Instrument and Remarks	Sanitization Procedure
1. Config. PROM for FPGA 128Mb (16MB)	No	No	FPGA configuration, Board header, Module header, License storage, FLASH file system.	WDIF	None; this is not user accessible.
2. Flash Memory 64Mb (8MB)	Yes	No	Board header, Receiver calibration data (User and Factory)	Down-converter	User calibration data can be reset.
3. FPGA 4Mb (512KB)	No	No	FPGA configuration	Down-converter	None; this is not user accessible.
4. Flash Memory 4Mb (512KB)	No	No	Board header, RFIO board header	Power Supply	None; this is not user accessible.
5. Flash Memory 64Mb (8MB)	Yes	No	Board header, Receiver calibration data (User and Factory)	Modulator	User calibration data can be reset.
6. FPGA 4Mb (512KB)	No	No	FPGA configuration	Modulator	None; this is not user accessible.
7. Config. PROM for FPGA 128Mb (16MB)	No	No	FPGA configuration, Board header, Module header, License storage, FLASH file system	BBG	None; this is not user accessible.

Table 5-3 Summary of TRX instrument memory

Memory Component, Type and Size	User Modifiable (Y/N)?	Volatile (Y/N)?	Purpose/Contents	Location in Instrument and Remarks	Sanitization Procedure
8. DRAM 4 GB DDR2	Yes	Yes	Signal data captured	WDIF	Cycle power.
8. DRAM 4 GB DDR2	Yes	Yes	Signal data for playback	BBG	Cycle power.



6 Memory Clearing, Sanitization and/or Removal Procedures

This section explains how to clear, sanitize, and remove memory from your instrument, for all types of non-volatile memory that can be written to during normal instrument operation.

Instrument Sanitization Procedures

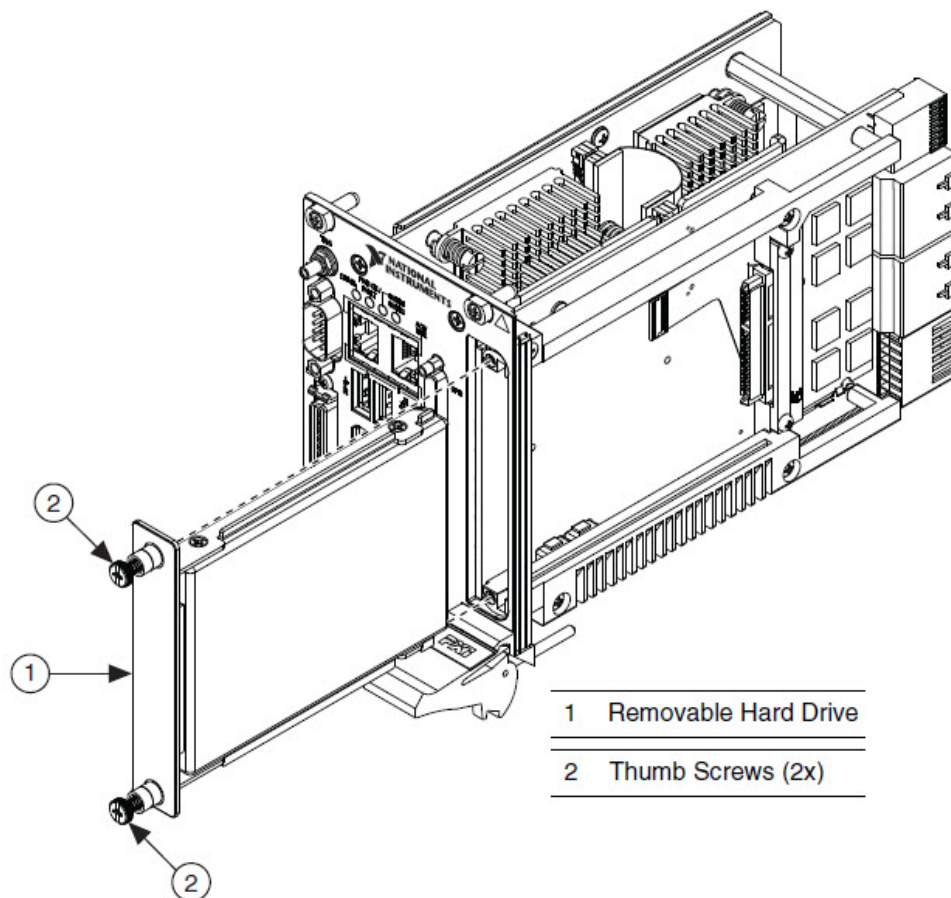
Removable Hard Drive Data Destruction

Several commercially available software programs exist to completely destroy all data on a data storage device such as the removable hard drive. DoD 5220.22-M is a software based data sanitization method for total data destruction. The DoD 5220.22-M sanitization method was originally defined by the U.S. National Industrial Security Program (NISP) in the National Industrial Security Program Operating Manual (NISPOM). The process involves overwriting existing information on the hard drive (or other data storage device). Typically, this means writing a 0 (zero) to every addressable location on the device, verifying the write, writing a 1 (one) to every addressable location and verifying the write, and then writing a random character (in some cases writing a 97) to every addressable location and verifying the write. Using a DoD 5220.22-M sanitization (or a variant) prevents all software and hardware based data recovery methods from obtaining information from the SSD. The instrument's disk drive is divided at the factory into three visible partitions, labeled C:, D: and E:, plus a fourth hidden partition.

Hard Drive Removal

Because it is virtually impossible to completely and selectively erase all user data on a hard drive without also destroying the operating system, the best method for maintaining security when the controller must be removed from a secure area is to remove or replace the hard drive.

Figure 6-1 Removing the hard drive



1. Turn the PXIe chassis power off.
2. Remove the controller from the PXIe chassis.
3. Position the controller, top side up, on the workbench. Loosen the thumb screws.
4. Unseat the removable hard drive from the connector and remove it from the slot.
5. Store the hard drive in the original antistatic packaging when not in use to avoid damage.

Application License Key Storage

License keys for measurement applications are stored on the removable hard drive; if you need to replace the SSD, contact Agilent Customer Support for help with restoring these licenses.

Other Memories

Other Memories

Other memory devices in the E6640A are described in:

- [“Memory in the Frequency Reference” on page 15](#)
- [“Memory in the TRX” on page 16](#)

As these memory devices do not include user-accessible non-volatile memory, no sanitization procedure is required for any memory component except the removable hard drive.



7 User and Remote Interface Security Measures

This chapter discusses options that are available to you to control and configure remote access to the instrument, including:

- [SCPI/GPIB Control of Interfaces](#)
- [Operating System Security Features](#)
- [USB Interfaces](#). This topic includes information about how to set the instrument's USB ports to read-only.

IMPORTANT

Users are responsible for providing security for the I/O ports for remote access, by controlling physical access to the I/O ports. The I/O ports must be controlled because they provide access to most user settings, user states, and the display memory.

SCPI/GPIB Control of Interfaces

The GPIB command `LLO` (local lockdown) can be sent by the controller to disable operation of the instrument's front-panel keys and softkey menus.

However, sending the `LLO` command does **not** disable access to the instrument via its USB ports. For details of how to restrict the operation of the USB ports, see ["Configuring USB for Read-only" on page 28](#) below.

Operating System Security Features

The instrument's Windows operating system includes a variety of features that you can invoke or modify to enhance system security. These include the following:

- The ability to create custom user accounts, and assign different security levels to each account by adding it to an existing group. The group types predefined by Windows are: Administrator, Power User, User, Backup Operator, and Guest, but you can also define new group types.
- To provide additional protection for instruments that have a network (or internet) connection, the standard Windows Firewall is enabled by default.

Determining the Test Set's Operating System

- You can install standard third-party antivirus and spyware detection software designed for use with Windows XP or Windows 7, as appropriate for your test set's operating system. If your instrument uses a network (or internet) connection, this may be advisable.

CAUTION

Running any third-party program while making measurements may adversely affect the instrument's performance.

Details of all these features are provided in the "Windows Security" section of the [Agilent EXM Wireless Test Set: Getting Started Guide](#).

Determining the Test Set's Operating System

You can easily determine your instrument's operating system version as follows:

1. Using the instrument front-panel, press **System > Control Panel...**
2. The Windows Control Panel appears. From the menu at the top of the Control Panel window, select **Help > About Windows**.
3. The About Windows message box appears, displaying the installed version of Windows.

USB Interfaces

The instrument's Microsoft Windows operating system can be configured to improve the security of the USB interfaces. This section includes the following topics:

- ["Disabling or Enabling Autorun/Autoplay" on page 24](#)
- ["Configuring USB for Read-only" on page 28](#)

Disabling or Enabling Autorun/Autoplay

Autorun, and the associated **Autoplay**, are Windows features that assist users in selecting appropriate actions when new media and devices are detected. The Autorun feature is disabled in the instrument by default, for improved security, unless the Administrator account is running. (In Administrator mode, Autorun is enabled, to aid with program installation.)

The procedure for disabling and enabling AutoPlay depends on your instrument's operating system (either Windows 7 or Windows XP). To determine the operating system version of your instrument, see ["Determining the Test Set's Operating System" on page 24](#).

Windows 7

If your instrument has the Windows 7 operating system, you can disable or enable AutoPlay via the Control Panel. Open the Control Panel and select **Hardware and Sound > AutoPlay**, then uncheck or check the "Use AutoPlay for all media and devices" checkbox.

If you want to understand details of how this AutoPlay setting affects the Windows Registry, see the [“Windows XP” on page 25](#).

Windows XP

You can change the Autorun configuration by editing the value of one of two Windows Registry keys. The Windows Registry is a database that stores critical configuration information for the instrument’s operating system.

CAUTION	Exercise extreme caution whenever you edit the Windows Registry. Entering an incorrect Registry value, or accidentally deleting Registry keys, may have serious consequences that can prevent the system from starting, or require that you reinstall Windows. The instructions in “Disable & Enable Procedure” on page 26 below assume that you are familiar with the use of the Windows Registry Editor to modify Registry settings.
----------------	--

Registry Key Definitions

Autorun can be configured per-machine or per-user.

NOTE	If the per-machine Registry key is present, its settings override those of the per-user Registry key.
-------------	---

The Registry key that controls the **per-machine** Autorun settings is:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun

The Registry key that controls the **per-user** Autorun settings is:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutoRun

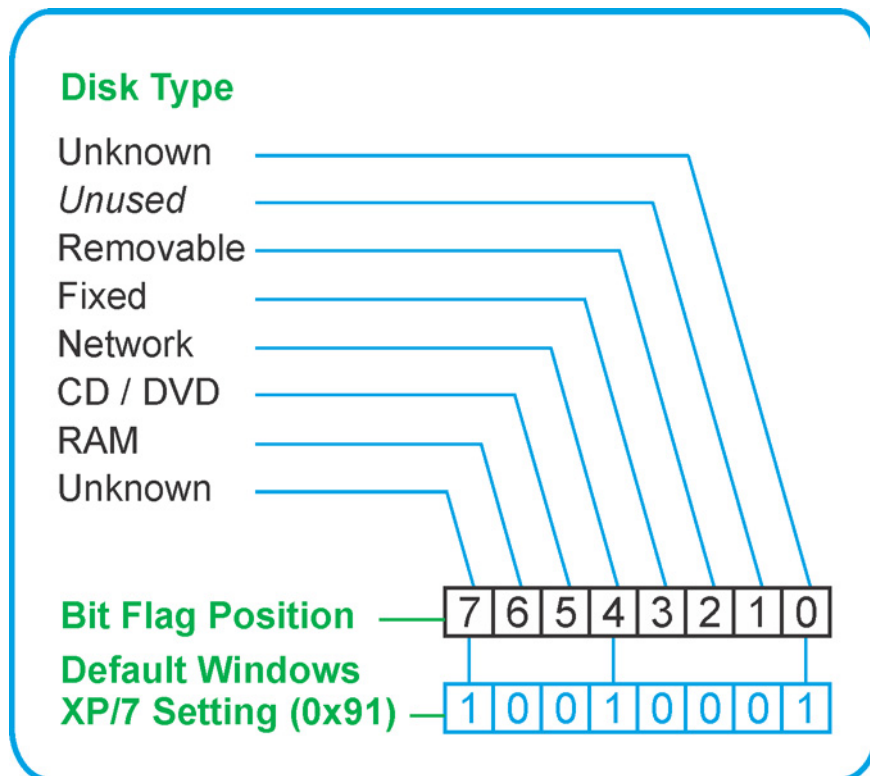
In the following discussions, we use the industry-standard abbreviation HKLM for the root key

HKEY_LOCAL_MACHINE, and the industry-standard abbreviation HKCU for the root key

HKEY_CURRENT_USER.

The DWORD value of either of these entries represents a set of single-bit flags. Each flag specifies the Autorun setting for a specific drive type, as shown in [Figure 7-1](#). Setting a bit flag to 1 disables Autorun for that drive type.

Figure 7-1 *Autorun Flag Definitions for NoDriveTypeAutoRun Registry entry*



As shown in [Figure 7-1](#) above, the default Windows XP (post-SP2) and Windows 7 value for this entry is 0x91 (under the entry HKCU\... \NoDriveTypeAutoRun). This setting disables Autorun for Unknown and Network drives, but enables Autorun for Removable, Fixed, CD/DVD or RAM drives.

You can disable Autorun for all drive types by changing the value to 0xFF, as described in the following section.

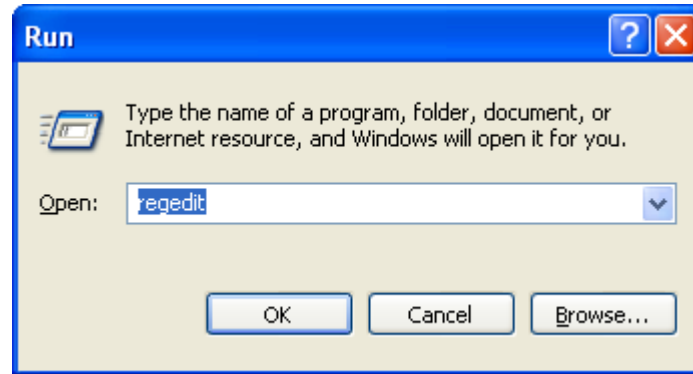
Disable & Enable Procedure

In view of the interaction between the per-machine and per-user Registry settings, as described above, it is recommended that, if both keys exist in your instrument's Registry, you should alter the settings of **both** Registry keys to the same value at the same time.

Use the following procedure to disable Autorun for all drive types, or to revert all Autorun settings to their Windows XP or Windows 7 default values. (Note that if your test set has a Windows 7 operating system, there is a simpler way to do this via the Control Panel; see ["Windows 7" on page 24](#).)

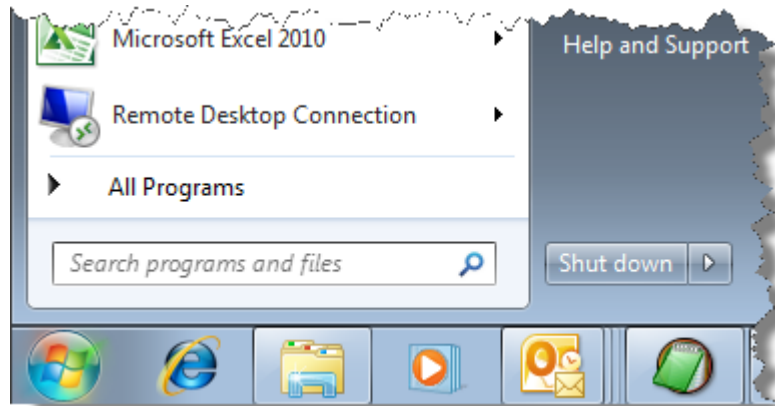
1. Open the Windows Registry editor, using one of the following methods (depending on your test set's operating system):
 - a. For Windows XP, select **Run...** from the Windows Start menu. Then, type `regedit` into the Windows Run dialog box, as shown in [Figure 7-2](#) below, and click **OK**.

Figure 7-2 Windows XP Run Dialog



- b. For Windows 7, click the Windows **Start** button at the bottom left of the screen. Type `regedit` into the **Search programs and files** box, as shown in Figure 7-3 below, then press **Enter**.

Figure 7-3 Windows 7 Search Box



2. The Registry Editor window appears. Using the tree view control on the left of the window, navigate to the per-machine (HKLM) key:
`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`.
3. To **disable** Autorun for all drive types, set the value of entry `NoDriveTypeAutoRun` to `0xFF`.
To **revert** Autorun settings to the Windows default values, set the value of entry `NoDriveTypeAutoRun` to `0x91`.
4. Again using the tree view control on the left of the Registry Editor window, navigate to the per-user (HKCU) key: `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer`.
5. To **disable** Autorun for all drive types, set the value of entry `NoDriveTypeAutoRun` to `0xFF`.
To **revert** Autorun settings to the Windows default values, set the value of entry `NoDriveTypeAutoRun` to `0x91`.
6. From the Registry Editor menu, select **File > Exit** to save the settings and exit the editor.
7. Shut down and restart the instrument, to enable the new settings to take effect.

Microsoft AutoRun Patch

NOTE

The information in this section applies only to Windows XP. If your test set has a Windows 7 operating system, you do not require this patch.

There is a defect in Windows XP that compromises the ability to disable Autorun. This defect has been fixed by a patch from Microsoft, as described in the [Microsoft Knowledge Base Article ID: 967715](https://support.microsoft.com/kb/967715).

This patch is included in the test set as shipped from the factory.

After the patch has been applied, there will be a Registry entry at:

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\HonorAutorunSetting with a default value of 1.

More Information

The following Wikipedia articles provide more information about AutoRun and AutoPlay:

<http://en.wikipedia.org/wiki/AutoRun>

<http://en.wikipedia.org/wiki/AutoPlay>

Configuring USB for Read-only

A convenient mechanism is provided to set the instrument's USB interfaces to read-only, thus preventing transfer of files from the instrument onto USB devices.

You can change this setting only when you are logged on as the Administrator. For details of how to log on to the instrument as the Administrator, see the [Agilent EXM Wireless Test Set: Getting Started Guide](#). To change the setting, do the following:

1. If you are **not** currently logged on to the instrument as the Administrator, you must log off.

If you are currently logged on to the instrument as the Administrator, and the Agilent XSA application is already running, go to Step 4.

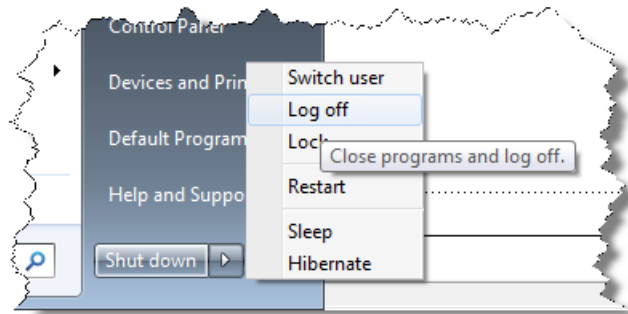
The log-off procedure executes more quickly if you first exit the Agilent XSA application, but you can also log off without exiting the application.
2. To log off, use one of the following procedures, depending on your instrument's operating system:
 - a. For Windows XP, select **Log Off** from the Windows XP Start menu (as highlighted in [Figure 7-4](#) below), then click **Log Off** in the Log Off Windows dialog that appears.

Figure 7-4 Log Off Button in XP Windows Start Menu



- b. For Windows 7, click the Windows **Start** button, then select **Shut down > Log off** from the Windows Start menu, as shown in [Figure 7-5](#) below.

Figure 7-5 Windows 7 Log off Control



3. After you have logged on to the instrument as the Administrator, restart the Agilent XSA application.
4. When the XSA application has fully initialized (that is, when the main results view and softkey menu are visible), press the **System** front-panel key.
5. From the System softkey menu, select: **More > Security > USB**.
6. Select the option **Read Only**.
7. To activate the configuration change, either log out and then back in under your usual user name (which by default is "instrument"), or cycle the instrument power.



8 Procedure for Declassifying a Faulty Instrument

Even if the instrument is not able to power on, it may be declassified by removing the disk drive from the instrument, using the appropriate procedure as described in [“Hard Drive Removal”](#) on page 20.



A: References

1. **DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)"**
United States Department of Defense. Revised February 28, 2006.
May be downloaded in Acrobat (PDF) format from:
http://www.dss.mil/isp/fac_clear/download_nispom.html
2. **ODAA Process Guide for C&A of Classified Systems under NISPOM**
Defense Security Service.
DSS-cleared industries may request a copy of this document via email, by following the instructions at:
<http://www.dss.mil/isp/odaa/request.html>
3. **Agilent EXM Wireless Test Set: Getting Started Guide**
Agilent Technologies Inc. 2013. Part Number: E6640-90001 (subject to revision).
A printed copy of this document is supplied with each instrument.
It is also available in Acrobat (PDF) form:
 - on the instrument's disk drive at the following location:
C:\Program Files\Agilent\SignalAnalysis\Infrastructure\Help\bookfiles\getstart.pdf
 - via download from:
<http://www.agilent.com/find/e6640a>
4. **Microsoft Knowledge Base Article ID: 967715**
"How to disable the Autorun functionality in Windows": may be viewed at:
<http://support.microsoft.com/kb/967715>
Note that a second article, at: <http://support.microsoft.com/kb/953252>, "How to correct 'disable Autorun registry key' enforcement in Windows", redirects to article ID 967715.

References

This information is subject to change
without notice.

© Agilent Technologies, Inc. 2014

Published in USA, January 2014

E6630-90005